(original) In a data processing system, a method comprising the steps of:

## IN THE CLAIMS

2 creating a migratable storage tree with a storage root key; and 3 creating a non-migratable storage tree with the storage root key, wherein the migratable 4 storage tree and the non-migratable storage tree are identically structured. 2. 1 (original) The method as recited in claim 1, wherein the migratable storage tree and the 2 non-migratable storage tree are created by a trusted computing module in accordance with 3 Trusted Computing Platform Alliance. 1 3. The method as recited in claim 1, wherein the migratable storage tree (original) 2 comprises migratable keys and a user key, wherein the non-migratable storage tree comprises 3 non-migratable keys and a user key. 1 4. (original) The method as recited in claim 1, wherein the non-migratable storage tree will 2 include non-migratable storage keys corresponding to each migratable storage key in the 3 migratable storage tree. 1 5. The method as recited in claim 1, wherein use authorization in the (original)

- 1 6. (original) The method as recited in claim 1, further comprising the steps of:
- 2 requesting a migratable storage key; and

1

2

1.

- 3 requesting a non-migratable storage key.
- 7. (original) The method as recited in claim 6, wherein the step of requesting a migratable storage key will identify a parent key in the migratable storage tree, and wherein the step of

non-migratable storage tree will be identical to use authorization in the migratable storage tree.

requesting a non-migratable storage key will identify a parent key in the non-migratable storage tree that corresponds to the parent key in the migratable storage tree.

8. (original) The method as recited in claim 1, further comprising the step of:

·1

2.

3

4

5

6

7

8

- when a key loading request is made for a migratable storage key, loading a key from the non-migratable storage tree instead of loading a corresponding key from the migratable storage tree.
- 9. (original) In a data processing system, a method comprising the steps of:
  - splitting a request to create a new migratable storage key with given authentication data and a first parent key into first and second commands;
  - wherein the first command creates a migratable storage key with the given authentication data and the first parent key; and
  - wherein the second command requests creating a non-migratable storage key with the given authentication data and a second parent key which is determined from looking up a key that corresponds to the first parent key in a database.
- 1 10. (original) The method recited in claim 9, wherein the migratable storage key and the non-migratable storage key are associated in a database.
- 1 11. (original) The method recited in claim 9, wherein the non-migratable key is a multi-2 prime key.
- 1 12. (original) The method recited in claim 9, where the non-migratable key is an elliptic curve key.

1	13.	(original) The method as recited in claim 9, further comprising the steps of:
2		creating a new migratable signing key with the given authentication data and a third
3	parent	key;
4		storing the new migratable signing key with the given authentication data and the third
5	parent	key;
6		storing the new migratable signing key with the given authentication data and a fourth
7	parent	key where the fourth parent key is a non-migratable key associated with the third parent
8	key in	a database.
1	14.	(original) The method as recited in claim 13, further comprising the steps of:
2		requesting a signature by the new migratable signing key;
3		searching the database for the location of a key blob containing the new migratable
4	signing key,	
5		loading a copy of the new migratable signing key stored in the key blob created with the
6	non-m	igratable parent key; and
7		signing with the new migratable signing key.
1	15.	(original) The method as recited in claim 9, further comprising the steps of:
2		creating a new data stored by means of the first parent key;
3		storing the new data with the first parent key;
4		storing the new data with the second parent key where the second parent key is a non-
5	migrat	table key associated with the third parent key in a database.
1	16.	(original) The method as recited in claim 15, further comprising the steps of:
2		requesting data stored by the new migratable storage key;
3		searching the database for the location of a key blob associated with the new migratable
4	storag	e key;

5 loading a copy of the key blob created with the non-migratable storage key, and 6 decrypting the data. 1 17. (original) The method as recited in claim 14, further comprising the steps of: 2 requesting migration of new migratable signing keys; 3 searching the database for the location of a key blob associated with a non-migratable 4 parent of the key to be migrated; 5 processing the migration. 1 18. (original) In a data processing system, a method comprising the steps of: 2 creating a migratable storage tree with a storage root key, and creating a non-migratable storage tree with the storage rootkey where the migratable 3 4 storage tree and the non-migratable storage tree are identically structured with corresponding 5 keys and authentication data. 1 19. (original) The method as recited in claim 18, wherein the migratable storage tree and the 2 non-migratable storage tree are created by a trusted computing module in accordance with 3 Trusted Computing Platform Alliance. 1 20. The method as recited in claim 19, wherein the migratable storage tree 2 comprises migratable keys and a user key, wherein the non-migratable storage tree comprises 3 non-migratable keys and a user key.

(original) The method recited in claim 18, wherein the migratable storage tree comprises

migratable keys and encrypted user data wherein the non-migratable storage tree comprises non-

1

2

3

21.

migratable keys and encrypted user data.

1 22. (original) The method as recited in claim 18, wherein the non-migratable storage tree

- will include non-migratable storage keys corresponding to each migratable storage key in the
- 3 migratable storage tree.

2

- 1 23. (original) The method as recited in claim 18, wherein the non-migratable storage tree
- will include non-migratable storage keys corresponding to a subset of the migratable storage
- 3 keys in the migratable storage tree.
- 1 24. (original) The method as recited in claim 18, wherein use authorization in the non-
- 2 migratable storage tree will be identical to use authorization in the migratable storage tree.
- 1 25. (original) The method as recited in claim 18, wherein use authorization in the non-
- 2 migratable storage tree can be deduced from user authorization in the migratable storage tree
- 3 with additional data.
- 1 26. (original) The method as recited in claim 25, wherein the use authorization in the non-
- 2 migratable storage tree is obtained by hashing the concatenation of the user authorization in the
- 3 migratable storage tree with a fixed string.
- 1 27. (previously presented) The method as recited in claim 1, wherein a migratable key can
- be transferred to other trusted platform module chips, and wherein a non-migratable key cannot
- 3 be transferred to other trusted platform module chips.